REMARKS

This amendment is responsive to the office action dated January 26, 2007. Claims 1-29 remain pending in the application. Claims 1, 26, and 29 are independent claims. As originally submitted, claim 1 of this application was not a step-plus-function claim (under 35 U.S.C. § 112, paragraph 6), and to make this even clearer that this claim is not a step-plus-function claim, claim 1 has been amended to recite the phrase "acts of" instead of the phrase "steps of."

Claims 1-29 stand rejected by the examiner. Assignee traverses the rejections of the claims.

Claim Rejections - 35 U.S.C. § 103

Claims 1-29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Dunnion et al. (U.S. Patent Application No. 2002/0199119) in view of Eldridge et al. (U.S. Patent No. 6,397,261). This rejection is traversed.

Claim 1 is directed to a method for handling secure message attachments for a mobile device. As support for examples of message attachments, assignee's specification discloses that the message attachments can be textual/word processing documents, image files, audio files, video files, etc. (See assignee's specification on page 13, lines 6-8.)

In claim 1, a server receives a second attachment provided within a secure message, wherein the secure message itself was received by the server as a first attachment. Based upon the mobile device requesting the second attachment, the server processes the secure message in order to locate within the secure message the second attachment. The second attachment is thereafter provided to the mobile device. (It is

noted that the amendment contained herein to claim 1 is to make more express what was inherent already in claim 1 – that is, the processing step is performed at the server.)

The office action maintains that claim 1 is unpatentable over Dunnion in view of Eldridge. Assignee respectfully disagrees. For example, none of the cited references disclose, suggest or motivate that the server processes the secure message in order to locate within the secure message the second attachment (as required by claim 1 in combination with the other limitations of claim 1). More specifically, such limitations of claim 1 are not disclosed in either paragraph 139, lines 1-20 of Dunnion or column 2, lines 26-30, 52-63 of Eldridge as maintained by the office action.

Paragraph 139, lines 1-20 of Dunnion provides:

> [0139] The decrypted message contains a signature that is now verified. The mail applet obtains the originator's public key from the server using the "Request user public key" function described in the table above. This key is used to verify the signature attached to the message. If this signature fails the user is informed that the message contents were not signed by the supposed originator of the message, thus providing authentication and non-repudiation. Another reason for the signature check to fail is that the message contents were altered, however in practice this cannot occur as the signature is wrapped in the encrypted content but it is included for future use (i.e. signed-only messages). The signature attachment is then removed from the message giving the unencrypted message composed by the originator. The mail applet then fills the relevant fields in a dialog box and displays the message. If the user requests that the message attachments be saved, the mail applet provides the user with a "Save File" dialog box for each attachment in turn, to allow selection of the directory and filename where the attachment is to be stored.

This passage from Dunnion is focused on client-side operations. As an illustration, this passage discloses that a client's mail applet checks the signature of a decrypted message. The client-side mail applet displays the message to the user; the mail applet also allows the user to save any message attachments. However, this passage lacks any disclosure

that the server processes the secure message in order to locate within the secure message the second attachment as required by claim 1.

Column 2, lines 26-30, 52-63 of Eldridge provides:

> In addition, it would be advantageous to provide an electronic mail system that supports secure transfer of document tokens between mail clients. Such a system would minimize the impact on data throughput of email servers when large files are attached to email messages.
> [...]
> Using the public key of the holder, the server authenticates the holder content of the document identifier. Also, the server verifies that the time stamp is within a predetermined window of time relative to a current time. Finally, the secure document server issues, to the holder of the document identifier, a copy of the document identified by the document identifier when the document token is authenticated. The authentication process allows the secure document server to authenticate a request for the document identified by the document token without prior knowledge of the identity of the holder of the document token.

These passages from Eldridge disclose a token-enabled server that uses digital signatures to provide secure transfer of document tokens between users. When the document token is authenticated by the server in Eldridge, a copy of the document as identified by the token is provided to the requester. Similar to Dunnion, these passages from Eldridge lack any disclosure that the server is processing the secure message in order to locate within the secure message the second attachment as required by claim 1. In other words, Eldridge is not processing a secure message in order to locate ***the attachment that is within the secure message*** so that that very attachment within the secure message can be sent back to a mobile device as required by claim 1. This lack of teaching in either Dunnion or Eldridge (whether viewed alone or in combination with each other) necessitates the removal of the instant rejection of claim 1 based upon these references.

Accordingly claim 1 is allowable and should proceed to issuance. Because claim 1 is allowable, its dependent claims are also allowable and should proceed to issuance.

Assignee respectfully disagrees with other positions of the office action. For example, assignee respectively disagrees with the rejection of claim 9. Claim 9 (which depends indirectly from claim 1) recites that a session key is received by the server from the mobile device for use by the server to decrypt the secure message. The office action maintains that such limitations of claim 9 are disclosed in Dunnion at paragraph 82, lines 1-14 and at paragraph 139, lines 1-20.

Paragraph 82, lines 1-14 of Dunnion is as follows:

> [0082] SSL is used between the web-server and the client PC in order to allow authentication of the server to the client. This prevents other sites masquerading as the valid server. In theory SSL provides encryption of data and therefore confidentiality, however, we assume that the protection afforded by SSL is weak. Therefore, all communications between the applet (registration or login) and the server begin by using the Diffie-Hellman algorithm to exchange a session key which is used to encrypt sensitive information before it is transferred over the SSL connection. Other key-exchange algorithms may be used in place of Diffie-Hellman without altering the basic design. The use of Diffie-Hellman may be seen in detail in a following section, which describes the registration and logon protocols in detail.

This passage from Dunnion only generally discloses that a session key is used to encrypt sensitive information between a web-server and a client PC. However there is no disclosure that the session key is being used for the specific purpose recited in claim 9 – that is in claim 9, the session key is for use by the server to decrypt the secure message which contains a second attachment that is to be sent to the mobile device. Dunnion itself remarks that it is the client-side mail applet that is performing secure message decryption and not the server (see Dunnion, paragraph 138, lines 1-11). With respect to the other cited passage from Dunnion, it was shown above that paragraph 139, lines 1-20

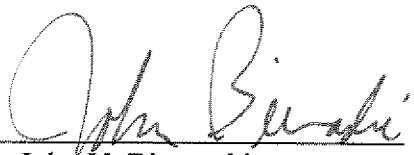
is disclosing client-side operations, and thus is not disclosing the server-side use of the session key as recited in claim 9. Because of such lack of disclosure in the cited references (whether viewed alone or in combination with each other), claim 9 is not rendered unpatentable by the cited references and should be allowed.

Assignee respectfully disagrees with the rejection of independent claims 26 and 29. As shown above, none of the cited references disclose, suggest or motivate that the secure message is processed at the server in order to locate within the secure message the second attachment as required by these claims (in combination with their other respective limitations). Accordingly claims 26 and 29 are allowable and should proceed to issuance. Furthermore because claim 26 is allowable, its dependent claims are also allowable and should proceed to issuance.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Respectfully submitted,

By: 

John V. Biernacki
Reg. No. 40,511
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939